NASA
Office of Inspector General

NASA's Software Asset Management

January 12, 2023 IG-23-008

Office of Inspector General

To report, fraud, waste, abuse, or mismanagement, contact the NASA OIG Hotline at 800-424-9183 or 800-535-8134 (TDD) or visit https://oig.nasa.gov/hotline.html. You can also write to NASA Inspector General, P.O. Box 23089, L'Enfant Plaza Station, Washington, D.C. 20026. The identity of each writer and caller can be kept confidential, upon request, to the extent permitted by law.

To suggest ideas or request future audits, contact the Assistant Inspector General for Audits at https://oig.nasa.gov/aboutAll.html.

NOTICE:

Pursuant to PL 117-263, section 5274, non-governmental organizations and business entities identified in this report have the opportunity to submit a written response for the purpose of clarifying or providing additional context to any specific reference. Comments must be submitted to HQ-Section5274Submissions@nasa.gov within 30 days of the report issuance date and we request that comments not exceed 2 pages. The comments will be appended by link to this report and posted on our public website. We request that submissions be Section 508 compliant and free from any proprietary or otherwise sensitive information.

RESULTS IN BRIEF

NASA's Software Asset Management

January 12, 2023 IG-23-008 (A-22-09-00-MSD)

WHY WE PERFORMED THIS AUDIT

NASA uses thousands of unique software products from hundreds of vendors in its efforts to advance science, technology, aeronautics, Earth studies, and space exploration. Each software application and program comes with a license—a contract between the entity creating or supplying the software and the end user—governing its use. Managing software licensing is deceptively complex due to the sheer volume of software vendors and applications yet is crucial to effectively secure NASA operations and track tens of millions of dollars in license fees. Software Asset Management is the business practice that administers the processes, policies, and procedures that support the software life cycle of planning, acquisition, use, management, and disposal.

Effective Software Asset Management helps reduce information technology (IT) costs and mitigate operational, cybersecurity, and financial risks related to software ownership and use. NASA's software portfolio consists of purchased software programs subject to varying types of licenses as well as internally developed mission and institutional software applications that are not licensed by the Agency. Purchased software must be used in accordance with the terms of its license with potential financial penalties if vendor audits find violations of license agreements or during the "true-up" process (the yearly vendor evaluation of qualified software licenses deployed within an organization). Internally developed software also needs to be tracked to identify duplicate or obsolete applications.

In this audit, we assessed whether NASA is managing its software assets in an effective and efficient manner while maintaining compliance with applicable requirements and security best practices. This included analyzing documentation relevant to NASA's software management activities, assessing NASA's centralized Software Asset Management program, and discussing internal software development activities with responsible officials.

WHAT WE FOUND

Software Asset Management practices at NASA currently expose the Agency to operational, financial, and cybersecurity risks with management of the software life cycle largely decentralized and ad hoc. Efforts to implement an enterprise-wide Software Asset Management program have been hindered by both budget and staffing issues and the complexity and volume of the Agency's software licensing agreements. We rated NASA's Software Asset Management as "basic"—the lowest of the four rating options in the Software Asset Management Maturity and Optimization Model developed by Microsoft and adopted from the International Organization for Standardization/International Electrotechnical Commission. Consequently, NASA is likely years away from moving to an enterprise computing model in which IT capabilities, such as software asset management and cybersecurity, are centralized and consolidated. In the meantime, the Agency has yet to embrace key best practices or fully implement federal guidance required to appropriately manage its Software Asset Management program.

NASA has not implemented a centralized Software Asset Management tool to discover, inventory, and track license data as required by federal policy. This shortcoming has resulted in NASA spending approximately $15 million over the past 5 years on unused licenses, an amount we found wasteful and are therefore questioning. We also found internally developed mission and institutional software applications suffer from a lack of centralization and inventory visibility, limiting the Agency's ability to identify duplicative or obsolete software. NASA's Software Asset Management policy is not comprehensive or standardized, leaving roles, responsibilities, and processes unclear. In addition, the Agency's Software Asset Management Office and Software Manager positions are misaligned and do not report to the Chief Information Officer as required by federal policy. The Agency also does not have consistent processes for legal representation during software contract negotiations and vendor audits, which can expose the Agency to increased costs because of penalties for violations of software license agreements. Furthermore, training for software license use and management is inconsistent across the Agency, with aging web-based training randomly assigned to personnel and a lack of a general software licensing training course available to the entire workforce.

NASA has failed to implement processes necessary to manage financial risks as software purchases are not sufficiently tracked and authorized by the Office of the Chief Information Officer (OCIO)—allowing some users to bypass OCIO authorization (and Software Asset Management team scrutiny) to purchase software through alternative means such as purchase cards. Moreover, NASA's current efforts to compile a complete and accurate report of annual software spending is a time consuming and mostly manual effort. Given all of these shortcomings, NASA has historically experienced a large influx of software into its network environment that is not sufficiently tracked for license compliance resulting in more than $20 million unnecessarily spent on software fines and penalties over the last 5 years. We estimate the Agency could have saved approximately $35 million ($20 million in fines and overpayments and $15 million in unused licenses) and moving forward could save $4 million over the next 3 years by implementing an enterprise-wide Software Asset Management program.

Lastly, NASA has not implemented the enterprise-wide processes necessary to appropriately manage the cybersecurity risks related to Software Asset Management. Software downloaded with privileged access is not tracked for license compliance and life-cycle management, and NASA does not have a consistent, Agency-wide process for limiting privileged access or using "least privilege" permissions, which gives users only the software permissions necessary for their job. This deviation from best practices is a cybersecurity risk because software deployed within the Agency raises both cybersecurity and software license compliance risks.

WHAT WE RECOMMENDED

To strengthen operational and cyber aspects of Software Asset Management, we recommended the Chief Information Officer (1) establish enterprise-wide (institutional and mission) Software Asset Management policy and procedures; (2) implement a single Software Asset Management tool across the Agency; (3) align the Agency Software Manager position to report to the Agency Chief Information Officer; (4) establish formal legal representation and guidance for vendor software audits; (5) establish a software license awareness training 'short course' focusing on approvals, compliance, and other issues a general user might encounter; (6) implement a centralized repository for NASA's internally developed software applications; and (7) develop an Agency-wide process for limiting privileged access to computer resources in accordance with the concept of least privilege. Additionally, to strengthen the financial aspects of NASA's Software Asset Management, we recommended the Chief Financial Officer (8) implement a "penalty spend" classification in SAP to track license infractions and true-up payouts and (9) centralize software spending insights to include purchase cards.

We provided a draft of this report to NASA management, who concurred or partially concurred with Recommendations 1, 2, 4, 5, 6, 7, 8, and 9. We consider the proposed actions responsive and therefore those recommendations are resolved and will be closed upon completion and verification of the proposed corrective actions. The Agency also partially concurred with Recommendation 3, however, we consider the proposed actions to this recommendation unresponsive. The Agency stated that the Software Asset Manager will establish a regular cadence of reporting to the Agency Chief Information Officer and senior management boards to provide insight into software management activities. We disagree that these actions meet the federal requirement for the software manager to report directly to the Chief Information Officer. Consequently, Recommendation 3 will remain unresolved pending further discussions with the Agency.

For more information on the NASA Office of Inspector General and to view this and other reports visit https://oig.nasa.gov/.

TABLE OF CONTENTS

Acronyms

BSA	BSA I The Software Alliance
CIO	Chief Information Officer
FY	fiscal year
IT	information technology
MEGABYTE	Making Electronic Government Accountable By Yielding Tangible Efficiencies
NIST	National Institute of Standards and Technology
NSSC	NASA Shared Services Center
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget

INTRODUCTION

Software—the applications, scripts, and programs used to operate computers and execute tasks—is integral to all of NASA's activities, from operations on Earth to missions to the Moon, Mars, and beyond. More than 49,000 Agency desktop, laptop, and engineering computers carry thousands of unique software products from hundreds of vendors, enabling NASA scientists and engineers to drive advances in science, technology, aeronautics, Earth studies, and human and space exploration. The Agency utilizes licensed software that ranges from Microsoft Office products like Outlook and Word to Ansys—modeling software used for solving complex mechanical problems such as manufacturing products in space through 3D printing.

Every piece of software including no-cost software comes with a license that governs its use. Software Asset Management is a business practice that administers the processes, policies, and procedures that support the software life cycle. That life cycle encompasses the planning, acquisition, use, management, and disposal of thousands of NASA software applications. Three important principles of Software Asset Management are:

- facilitating the discovery of software assets, whether installed on a user's computer or accessed via a remote cloud-based application;
- ensuring the validity of end user license agreements; and
- validating the appropriate use of free software.

What is a software license?

A software license is a contract between the entity that created and supplied an application, underlying source code, or related product and its end user. The license is a text document designed to protect the intellectual property of the software developer and to limit any claims against them that may arise from its use.

Effective Software Asset Management helps reduce information technology (IT) costs and mitigate operational, cybersecurity, and financial risks related to the ownership and use of software. An effective Software Asset Management program also gives IT managers a full view of their organization's software asset landscape. This information, if accurate and kept current, enhances configuration management, incident management, organizational governance, and cybersecurity practices.[1]

Leading groups in the cybersecurity field have touted the importance of effective Software Asset Management. According to the National Institute of Standards and Technology (NIST), Software Asset Management can reduce the probability that attackers will find and exploit unmanaged software through the removal or prevention of unauthorized or unmanaged software. Likewise, a report from BSA I The Software Alliance (BSA)—a software trade group founded by Microsoft—stressed the

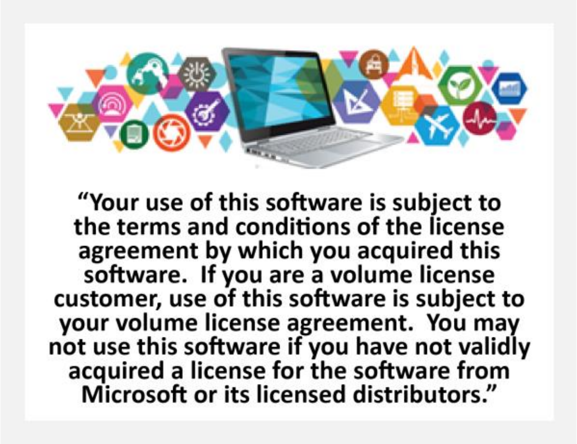
[1] Configuration management is the process of maintaining systems, such as computer hardware and software, in a desired state and ensures that systems perform in a manner consistent with expectations over time. Incident management is a series of steps taken to identify, analyze, and resolve critical IT-related incidents, which could lead to issues in an organization if not addressed. Organizational governance in IT is a formal framework that provides a structure for organizations to ensure IT investments support business objectives. Cybersecurity practices protect computer systems and data from unauthorized access.

important role Software Asset Management plays in cybersecurity.[2] The report states a network is at its greatest risk when unlicensed software is installed and unmanaged, and that lowering the incidence of unlicensed software ultimately reduces cybersecurity risk.

In this audit, we assessed whether NASA is managing its software assets in an effective and efficient manner while maintaining compliance with applicable requirements and security best practices. See Appendix A for details on the audit's scope and methodology.

Background

Managing software licenses has long been an important, if sometimes overlooked and unappreciated, task for IT departments. Over time, the stakes in software compliance have risen as license types increase and become more complex, and as vendor audits occur more frequently.[3] Since software is considered creative work akin to music, movies, and books, it is protected by U.S. copyright laws and the use or distribution of unauthorized software is illegal.[4] As such, organizations are responsible for enforcing adherence to copyright laws and are held liable if found in violation. A typical Microsoft end user license agreement warning is depicted in the box to the right.



"Your use of this software is subject to the terms and conditions of the license agreement by which you acquired this software. If you are a volume license customer, use of this software is subject to your volume license agreement. You may not use this software if you have not validly acquired a license for the software from Microsoft or its licensed distributors."

A software license violation penalty is the fine or legal action that occurs as a result of the unauthorized use, duplication, or distribution of copyrighted software by an individual or organization, also known as software piracy. The risks of software piracy have not only legal implications that can cost hundreds of thousands of dollars, but also create a cybersecurity risk to an organization's IT systems. According to the BSA, about 40 percent of installed software products globally are illegally copied—shrunken IT budgets and the overall slowdown in technology spending has contributed to this phenomenon.

In almost all cases, software sold to users via a licensing agreement or subscription must be renewed periodically. NASA programs and offices, including the Office of Inspector General (OIG), primarily contract with an array of vendors such as Adobe, Microsoft, Oracle, IBM, PTC Windchill, SAP, and Splunk for proprietary software licenses to conduct business operations. Navigating vendor software license agreements is a complex process, frequently requiring collaboration between IT professionals and legal advisors specializing in technology and contract law. While license agreements differ depending on the vendor, platform, and contract, commonly used categories are listed below.

[2] BSA attempts to eliminate software piracy (reproduction or use of unlicensed software). The group's membership includes NASA vendors such as Adobe, Microsoft, Oracle, PTC Windchill, SAP, and Splunk. BSA, *Unlicensed Software and Cybersecurity Threats* (January 2015).

[3] A vendor software license audit compares the number of licenses an organization has purchased with the number of computers in which the software is currently installed. Software license agreements almost always include language that allows the vendor to audit a customer's use of the software to determine compliance with the license agreement.

[4] Copyright Act of 1976, Pub. L. No. 94-453 (1976), codified at 17 U.S.C.

- *Fee per device*. Each device (mobile or desktop) is charged a fee to access the software. Installation is restricted to a particular computer. MATLAB, a programming platform used by engineers and scientists to analyze data, develop algorithms, and create models, is an example of fee-per-device licensing.
- *Fee per user*. Each user is charged a fee to access the software. The user can typically use multiple devices at their discretion. SAP, financial management software used at NASA, is an example of fee-per-user licensing.
- *By network.* All machines linked to a network are granted access to the software. Symantec Endpoint Protection, a security software suite for server, desktop, and laptop computers, is a common example of network licensing.
- *Subscription*. Fees are charged either by user or device, or some combination of the two. Access is limited to the term of the subscription, typically a year. A Microsoft 365 Enterprise Agreement is an example of subscription licensing.
- *Public*. This type of license is for software known as freeware that can be used, modified, shared, or copied without limitation. The Linux operating system, software that manages the hardware resources associated with a user's computer, is an example of a free public license.
- *Permissive*. Similar to a public license, this type of license may contain limited restrictions on how the user may modify or distribute the software. Node.js—a platform for executing JavaScript, the programming language used to create and control dynamic website content that moves, refreshes, or changes on the screen—uses a permissive license.
- *Database.* These licenses may be linked to a number of devices and can include a specified number of servers connected to databases. Oracle is an example of database software that requires licensing.
- *Metered/Consumption-based*. The software vendor charges licensing fees based on how frequently users access specific application features, data, or other resources. Software vendors can measure factors such as total use time, number of database queries, number of processing cycles consumed, or quantity of stored data, and charge customers accordingly based on how they used the software. Amazon Web Services, commonly known as cloud computing, is an example of consumption-based licensing.[5]

An overview of the software products and vendors referenced in this report can be found in Appendix B.

Federal Guidance

In June 2016, the Office of Management and Budget's (OMB) software licensing policy required federal agencies to appoint a software manager who reports to the Chief Information Officer (CIO) and is responsible for managing agency-wide commercial and commercial off-the-shelf software service agreements and licenses.[6] Furthermore, the policy specifically mentions Software Asset Management tools, software license optimization tools, continuous diagnostics and mitigation tools, continuous

[5] Cloud computing is the practice of using a network of remote servers hosted on the internet for centralized data access and storage to computer services or resources.

[6] OMB Memorandum M-16-12, *Category Management Policy 16-1: Improving the Acquisition and Management of Common Information Technology: Software Licensing* (June 2, 2016). Commercial off-the-shelf software are products commercially ready-made and available for sale, lease, or license.

monitoring as a service, network management tools, and finance and accounting systems to report on software inventory, prices, and usage.[7]

In July 2016, the Making Electronic Government Accountable By Yielding Tangible Efficiencies (MEGABYTE) Act of 2016 required agencies to establish and manage a software license inventory.[8] The objective was to capture cost savings through better software license management and deeper analysis of license inventory. The MEGABYTE Act also required CIOs to develop a comprehensive software licensing policy, including requirements to:

- Establish a comprehensive inventory, including 80 percent of software license spending and enterprise licenses in the executive agency, by identifying and collecting information about software license agreements using automated discovery and inventory tools.
- Regularly track and maintain software licenses to assist the agency in implementing decisions throughout the software license management life cycle.
- Analyze software usage and other data to make cost-effective decisions.
- Provide training relevant to software license management.
- Establish goals and objectives of the software license management program of the executive agency.
- Consider the software license management life-cycle phases to implement effective decision-making and incorporate existing standards, processes, and metrics.

Finally, in September 2020, NIST issued a special publication on security and privacy controls that specified an organization should employ automated mechanisms to maintain an up-to-date, complete, accurate, and readily available inventory of information system components.[9] For example, inventory information should include software license data, software version numbers, component owners, and—for network components or devices—machine names and network addresses. NIST also noted that organizations should use software in accordance with contract agreements and copyright laws and track the use of software protected by quantity licenses to control copying and distribution.[10]

[7] Software Asset Management tools provide an automated process to support tasks required to produce and maintain compliance with software vendor license use rights and improve an organization's ability to optimize software risk and spend. Software license optimization tools proactively manage an organization's software assets to ensure the right types of licenses are procured, maximize the utilization of assets and compliance with the terms of the licenses, and minimize unplanned costs. Continuous diagnostics and mitigation tools find cybersecurity risks on an ongoing basis and prioritize and focus on these risks based on potential impacts. Continuous monitoring technology provides real-time feedback on the overall health of IT infrastructure. Network management tools may help locate devices and computers connected to a network, find errors or other issues, track activity, and improve security.

[8] Making Electronic Government Accountable By Yielding Tangible Efficiencies Act of 2016, Pub. L. No. 114-120 (2016).

[9] NIST Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (September 2020).

[10] Quantity or volume licensing is a special type of software licensing that uses a single license key to authorize the software on multiple computers.

Best Practices for Managing Software Licenses

Overseeing thousands of software licenses—tracking who is using them, ensuring license fees are up-to-date, and assessing the license agreement terms—can be daunting and time-consuming. According to government and industry experts including NIST, Microsoft, and the International Organization for Standardization, a considered effort to proactively manage agency software assets includes establishing a program empowered by senior management, consists of multi-departmental team members, and utilizes Software Asset Management software that integrates and normalizes data for software inventory, usage, and license reconciliation.[11]

The *Software Asset Management Maturity and Optimization Model* provides organizations with a way to benchmark their current ability to manage software.[12] The model classifies Software Asset Management into 10 key competencies (described in Appendix C), with each competency assessed one of four possible ratings:

- *Basic.* Software is managed on an ad hoc basis with few, if any, comprehensive policies.
- *Standardized.* The agency uses a discovery tool or data repository for tracking assets, although the information may not be complete or accurate enough for decision-making.
- *Rationalized.* Assets are actively managed, and the agency has put in place policies, procedures, and tools integrated into the full IT asset life cycle.
- *Dynamic.* Assets are optimized, with near real-time alignment with changing business needs.

Building the right Software Asset Management team is critical to the success of license management. Ideally, representatives across NASA from the Office of the Chief Information Officer (OCIO), procurement, legal, and finance would join together to strengthen the Agency's management and compliance throughout its IT ecosystem and contribute to a successful and proactive Software Asset Management program.

Adopting software management best practices—proven methods, processes, techniques, and activities that organizations define and use to minimize risks and maximize the chances of success—ensures assets are managed appropriately and helps minimize risks by ensuring the software is used in compliance with licensing agreements. For example, centralizing license processing, identifying and tracking inventory, analyzing license data, and training can help create an IT environment where software license compliance is part of a broader strategic effort for IT asset management.

[11] The International Organization for Standardization is a global network of experts that represent a wide range of sectors, from soap to spacecraft to coffee, to implement internationally recognized industry standards. This includes the areas of cybersecurity and Software Asset Management. Data normalization is the process of organizing data by adopting consistent formatting, standardizing data entry, and removing duplicate data.

[12] The Software Asset Management Maturity and Optimization Model was developed by Microsoft and adopted from International Organization for Standardization/International Electrotechnical Commission 19770-1:2012 Software Asset Management processes.

Software Life Cycle and Organizational Responsibilities for Software Asset Management

The software life cycle—plan, acquire, use, manage, and dispose—has multiple overlapping parts. Broadly, NASA's Office of the Chief Engineer is responsible for protecting the Agency's investment in software products and ensuring that the government has clear rights and the appropriate license to use the software.[13]

Software Management Life Cycle
Plan
Acquire
Use
Manage
Dispose

The Office of Procurement plays a key role in the acquisition phase, as Agency software is purchased through various General Services Administration and NASA's Solution for Enterprise-Wide Procurement contracts.[14] Centralized acquisition simplifies licensing management—ensuring visibility of the software landscape by optimizing value and controlling cost. But the brunt of the work occurs in the management phase, which involves monitoring usage, licensing compliance, and software entitlement visibility.[15] Since software assets are intangible, they are harder to track than physical hardware components. Managing software licensing is deceptively complex—for NASA, the OIG, and other agencies—considering the hundreds of software vendors and thousands of applications or environments that span from on-premises locations at NASA facilities to the cloud.[16] This makes detecting non-compliance, over usage, and cost trends difficult. Just as an example, every month NASA uses 1.5 million hours of cloud computing, employing over 2,500 physical servers and over 7,000 virtual servers all with various software and licensing considerations supporting approximately 35,000 users.

At NASA, responsibility for the management of software assets falls under multiple offices, including those focused on IT and procurement.[17] Within the OCIO, NASA's Enterprise Business Management Office houses the Software Asset Management Office and its Agency Software Manager who is responsible for providing centralized oversight, guidance, and management of NASA's software license portfolio; this includes ensuring operational and financial risks are addressed throughout the product life cycle. Separately within OCIO's Service Management Office, the End User Support Office assists with software acquisition, implementation, and administration across the Agency's enterprise (institutional

[13] NASA Procedural Requirements 7150.2D, *NASA Software Engineering Requirements* (March 8, 2022). In this audit, we focus on the acquisition and management of software.

[14] NASA's Solution for Enterprise-Wide Procurement consists of over 140 pre-competed prime contract holders, including more than 100 small businesses that provide IT products and services for federal agencies and their approved contractors.

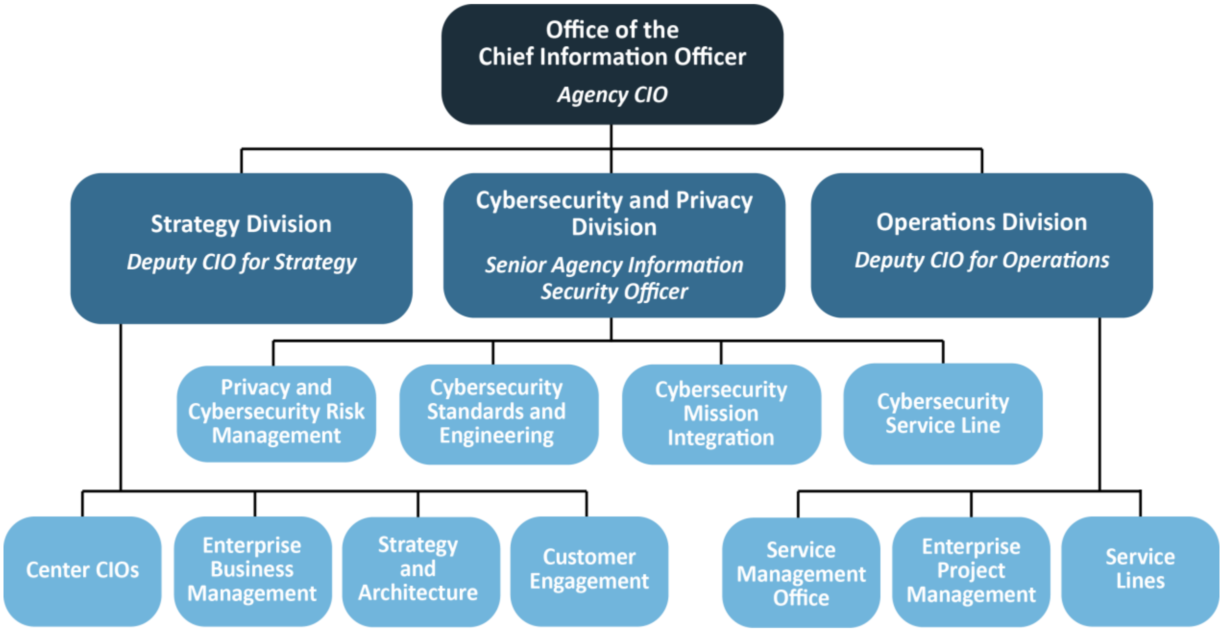
[15] Similar to a license, an entitlement is the right to use and/or access software as defined through agreement(s) with the software vendor.

[16] NASA's primary facilities consist of a Headquarters office in Washington, D.C.; nine geographically dispersed Centers; and the Jet Propulsion Laboratory, a federally funded research and development center operated under contract by the California Institute of Technology located near Pasadena, California.

[17] NASA's IT assets generally fall into two broad categories: institutional and mission. Institutional systems include desktop and laptop computers, enterprise business applications, web services, data centers, and networks. Mission systems support the Agency's aeronautics, science, and space exploration programs. While the OCIO has responsibility for institutional systems, mission directorates fund their own networks and IT personnel; therefore, in most cases, mission personnel rather than OCIO staff have visibility over the operational and security aspects of mission networks.

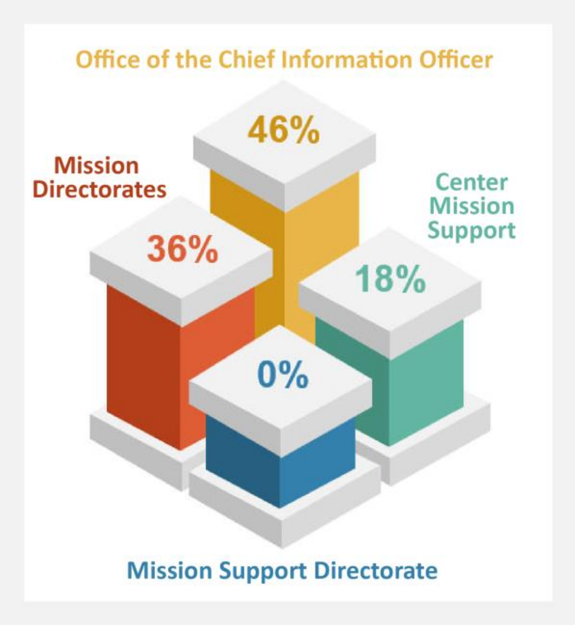
and mission) IT systems. Additionally, independent of OCIO responsibility, the Office of Procurement's Enterprise License Management Team—located at the NASA Shared Services Center (NSSC)—provides software support to the OCIO for enterprise license agreements such as Microsoft, Oracle, and IBM, and procurements exceeding $250,000. Figure 1 depicts the OCIO organization.

Figure 1: Office of the Chief Information Officer Organization Chart


Office of the Chief Information Officer
Agency CIO
Strategy Division
Deputy CIO for Strategy
Cybersecurity and Privacy Division
Senior Agency Information Security Officer
Operations Division
Deputy CIO for Operations
Privacy and Cybersecurity Risk Management
Cybersecurity Standards and Engineering
Cybersecurity Mission Integration
Cybersecurity Service Line
Center CIOs
Enterprise Business Management
Strategy and Architecture
Customer Engagement
Service Management Office
Enterprise Project Management
Service Lines

Source: NASA OIG presentation of the Agency's OCIO organization.

Note: The Agency Software Manager falls under the Enterprise Business Management Office.



To further improve its operations, the OCIO is currently working through a transformation initiative—an outcome of the Agency's Mission Support Future Architecture Program that sought to move mission support services traditionally managed at each NASA Center and headquarters, including IT, human capital, and financial management, to an Agency-wide, enterprise operating model. Specifically, the OCIO is moving the Agency toward an enterprise computing model that centralizes and consolidates IT capabilities, including software management and cybersecurity.

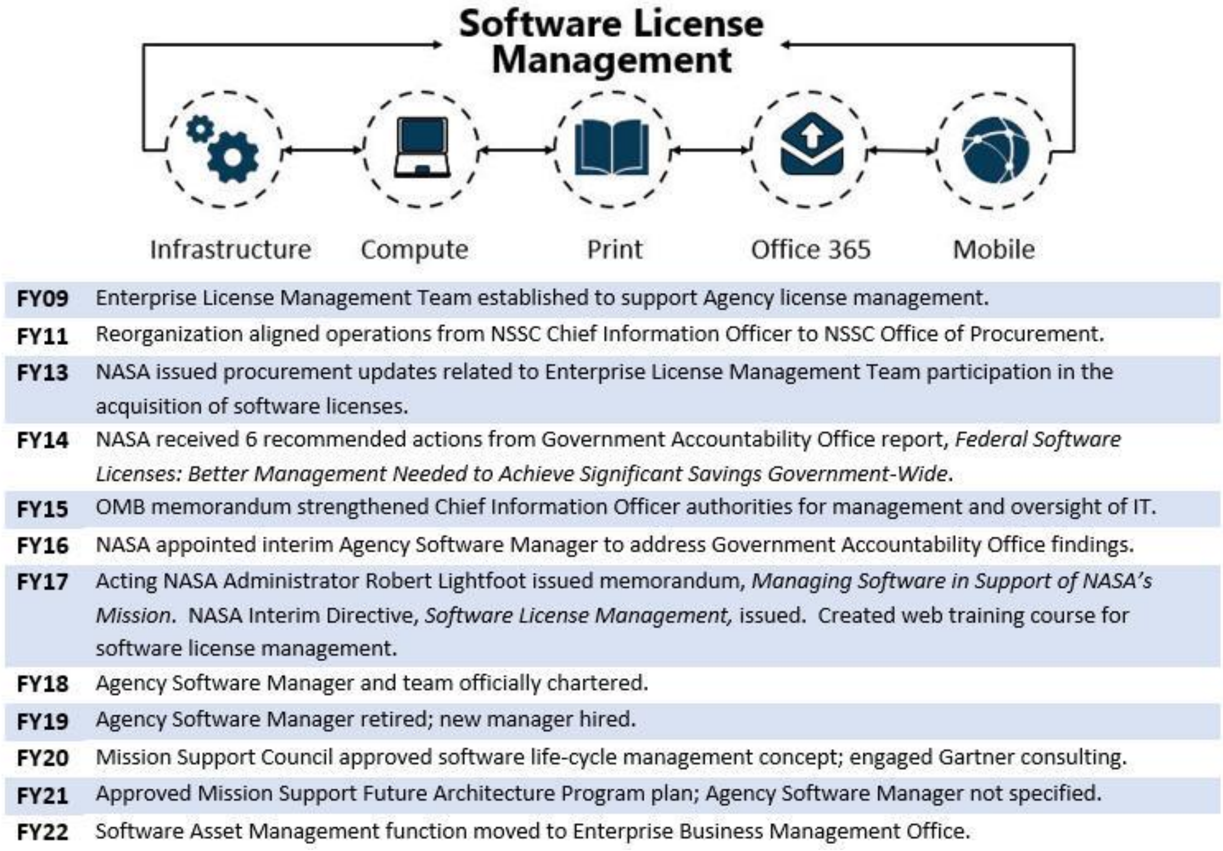
However, the transformation to an enterprise computing model is years away. For now, as depicted in the graphic, separate from the OCIO, Mission Directorates and Center Mission Support together control more than half—approximately 54 percent—

of the Agency's IT assets, including software purchasing and asset life-cycle management for their mission-related projects.[18]

Key Milestones in NASA's Software Asset Management Efforts

As shown on Figure 2, NASA began to focus on Software Asset Management during fiscal year (FY) 2009.

Figure 2: Timeline of NASA's Software Asset Management Efforts



FY09	Enterprise License Management Team established to support Agency license management.
FY11	Reorganization aligned operations from NSSC Chief Information Officer to NSSC Office of Procurement.
FY13	NASA issued procurement updates related to Enterprise License Management Team participation in the acquisition of software licenses.
FY14	NASA received 6 recommended actions from Government Accountability Office report, *Federal Software Licenses: Better Management Needed to Achieve Significant Savings Government-Wide*.
FY15	OMB memorandum strengthened Chief Information Officer authorities for management and oversight of IT.
FY16	NASA appointed interim Agency Software Manager to address Government Accountability Office findings.
FY17	Acting NASA Administrator Robert Lightfoot issued memorandum, *Managing Software in Support of NASA's Mission*. NASA Interim Directive, *Software License Management,* issued. Created web training course for software license management.
FY18	Agency Software Manager and team officially chartered.
FY19	Agency Software Manager retired; new manager hired.
FY20	Mission Support Council approved software life-cycle management concept; engaged Gartner consulting.
FY21	Approved Mission Support Future Architecture Program plan; Agency Software Manager not specified.
FY22	Software Asset Management function moved to Enterprise Business Management Office.

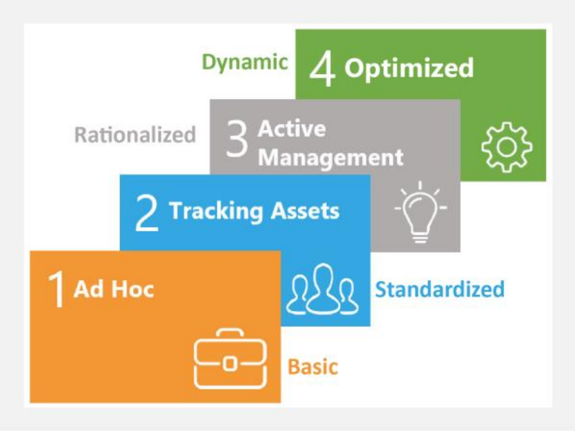
Source: NASA OIG presentation of Agency information.

[18] NASA has six Mission Directorates: Aeronautics Research, Exploration Systems Development, Science, Space Operations, Space Technology, and Mission Support. The Mission Support Directorate manages mission functions such as IT, legal, and procurement—consisting of 552 IT assets equating to 0 percent on our chart.

Significant Shortcomings Stymie NASA's Software License and Asset Management Activities

Software license management is a blind spot at NASA, exposing the Agency to operational, financial, and cybersecurity risks. Specifically, we found that NASA's management of its software life cycle remains decentralized and ad hoc with the Agency's efforts to implement an enterprise-wide Software Asset Management program challenged by budget and staffing issues as well as the complexity and volume of its software licensing agreements. For example, even though the Agency has been working on enterprise license management for more than 10 years, its efforts have not progressed past the early stages of maturity due to funding and staffing shortfalls. Instead, NASA continues to use a basic ad hoc approach to Software Asset Management that presents numerous risks, adds to costs, and is likely unsustainable. Consequently, NASA software assets are not well monitored, and the Agency does not know whether its software licenses are under- or over-subscribed, resulting in significant unidentified liabilities or underutilized assets as well as millions of dollars owed to software vendors.

NASA has not embraced key best practices or fully implemented federal guidance required to appropriately manage operational risks related to Software Asset Management. Using the Software Asset Management Maturity and Optimization Model, we evaluated NASA's ability to manage software against key best practices including regularly tracking and maintaining comprehensive inventories, analyzing software license data to inform investment decisions, and reconciling entitlement records against vendor data. In our view, NASA's Software Asset Management is rated as Basic—the lowest of the four rating options—given that the Agency's software is managed on an ad hoc basis with few comprehensive policies. See Appendix C for additional information about the maturity and optimization model.



Operational Deficiencies

Deficient Software License Management Practices

NASA continues to struggle to achieve effective operational control over thousands of unique software products from hundreds of vendors used throughout the Agency's institutional and mission IT ecosystem. Although the MEGABYTE Act requires agencies to establish a comprehensive inventory and regularly track and maintain software licenses during the software license management life cycle, we found NASA has not implemented a centralized Software Asset Management tool to discover, inventory, and normalize license data.[19] Rather, NASA uses BigFix, a centralized operating system patch management service, to provide cyber vulnerability visibility and manage patch compliance but not for license inventory.[20] While BigFix provides visibility into deployment data—software on the network—it does not provide a complete picture or visibility into all Agency IT software assets. The granular information necessary to analyze software data such as entitlement (right to use) and consumption (utilization) compliance is not provided by the application. Consequently, NASA's ability to reconcile inventory and normalize entitlement data against deployment data is limited, requiring a labor-intensive manual effort to assess compliance and the risk posture of each piece of software.

Oracle Overspend

The Agency does not have a centralized, authoritative database or inventory that tracks what licenses have been purchased, specific licensing agreements, and whether licenses are available for use by others at the Agency. These shortcomings have resulted in NASA spending approximately $15 million over the past 5 years on unused Oracle licenses. While this is just one example, in our view there are likely multiple others unknown to the Agency. OCIO officials explained that long-standing problems with tracking acquisition and utilization of Oracle software licenses made it difficult to control costs and complicated efforts to negotiate new enterprise agreements with Oracle. Two historical scenarios contributed to the overspend on unused licenses:

1. *Vendor lock-in*. A situation in which a customer using a product or service cannot easily transition to a competitor's product or service. NASA purchased large amounts of Oracle products to support Space Shuttle processing and other mission operations during that timeframe containing licensing terms that made transitioning to a competitor difficult due to proprietary technologies.
2. *Status-quo renewal*. NASA has been unwilling to risk a license audit by Oracle because of the lack of solid, centralized visibility into deployment and use of the software. OCIO officials explained that they "knew better than to try our luck with an audit." Simply put, merely the potential threat of being audited by the vendor encouraged overbuying when the accuracy of Agency Software Asset Management was suspect.

OCIO officials we spoke with acknowledged the potential benefits of implementing a central source for information on software entitlements—the right to use or access software—and they are committed to fully addressing the current Oracle overspend situation. In preparation for the Oracle contract renewal in April 2023, the OCIO, along with the Enterprise License Management Team, are gathering requirements and examining 'how and why' Oracle licensing became so cumbersome and complex to manage. In parallel, the Agency is also reviewing the current and desired licensing environment to quantify the true cost of doing business with Oracle. While we are encouraged by these efforts, the $15 million spent over the past 5 years on unused Oracle licenses was wasteful and therefore we are questioning these costs. See Appendix D for our analysis of these questioned costs.

Internally Developed Applications

While Oracle is a commercial software product, internally developed mission and institutional software applications suffer from a similar lack of centralization and inventory visibility. OCIO officials explained

[19] Pub. L. No. 114-120.

[20] A patch is a quick repair of programming designed to resolve functionality issues, improve security, or add new features.

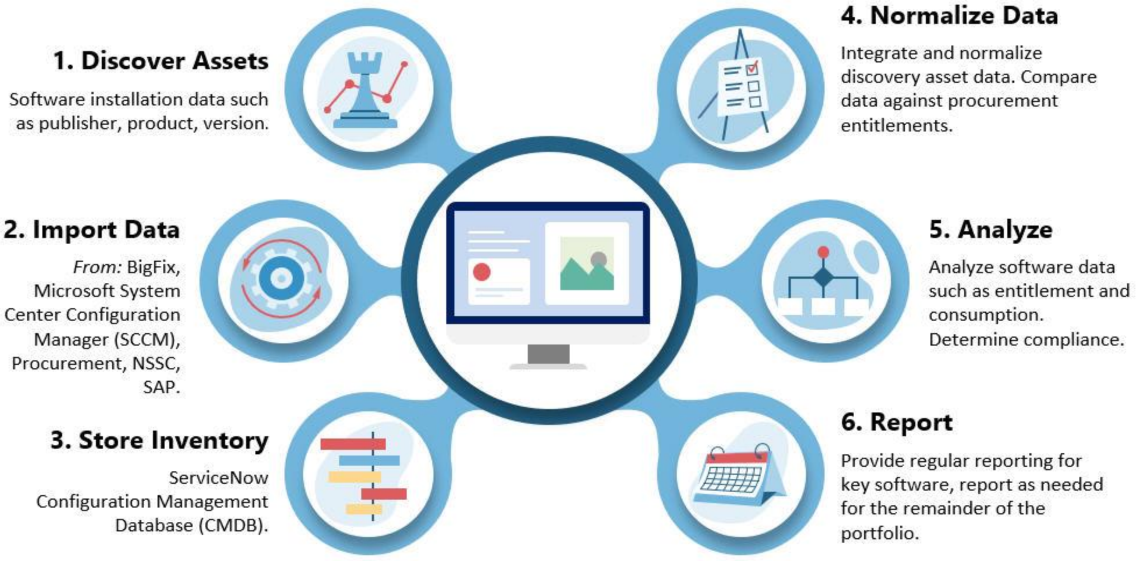
that the Agency does not have consistent processes or policies in place for software rationalization—the method of identifying existing applications to determine if they are needed, duplicative, or obsolete.

NASA's authoritative source for inventorying internally developed software is a rationalization application known as the Agency Application Rationalization Tool. Although this tool attempts to fill a void by identifying duplicate or obsolete applications, it is not used consistently across the Centers nor is it currently funded or staffed for full operational capability. Without a comprehensive software inventory that catalogs existing, duplicate, and obsolete software, NASA's ability to identify waste or potential cost savings for internally developed applications is limited. While the Agency does not internally "license" software for use, a comprehensive inventory could reduce instances of duplicative development, such as cloud-based applications, that left unaddressed could result in the misuse of commercial software license agreements.

Software Asset Pilot Program

To its credit, the OCIO has recently begun an initiative to address asset management by funding the purchase and implementation of the Software Asset Management component of ServiceNow—an application that tracks, evaluates, and manages software licenses, compliance, and optimization. A collaborative effort between OCIO and the NSSC, this pilot program will evaluate the integration of the Software Asset Management workflow into the NSSC's existing ServiceNow environment.[21] The NSSC estimates implementing the pilot framework in April 2023. Figure 3 depicts a simplified Software Asset Management workflow that NASA will use during the pilot program.

Figure 3: Simplified Software Asset Management Pilot Program Workflow


1. Discover Assets
Software installation data such as publisher, product, version.
2. Import Data
From: BigFix, Microsoft System Center Configuration Manager (SCCM), Procurement, NSSC, SAP.
3. Store Inventory
ServiceNow Configuration Management Database (CMDB).
4. Normalize Data
Integrate and normalize discovery asset data. Compare data against procurement entitlements.
5. Analyze
Analyze software data such as entitlement and consumption. Determine compliance.
6. Report
Provide regular reporting for key software, report as needed for the remainder of the portfolio.

Source: NASA OIG presentation of NASA's Software Asset Management workflow.

OCIO officials explained that NASA is strategically rolling out the pilot program due to funding limitations and to allow time to develop the processes and skillset necessary to integrate complex software

[21] The NSSC uses ServiceNow's cloud-based service platform for managing human resources, finance, procurement, and IT-problem tracking.

management life-cycle activities into NASA's broader IT ecosystem. Focusing on NASA's largest and most critical software vendors such as IBM, Microsoft, and Oracle, the pilot program will seek to demonstrate how to make the best use of ServiceNow's integration capabilities with Agency IT, procurement, and finance data. The remaining vendors in the Agency's software portfolio will be added on an ad hoc basis.

While we are encouraged by this Software Asset Management pilot program, its success is dependent upon leadership commitment, adequate funding, and changes to the Agency's culture and processes including instituting better cooperation between the OCIO, Mission Directorates, and Centers. Currently, the Agency lacks an enterprise approach for managing both commercial and internally developed software. The capability to provide a single, integrated view of installed software to allow a one-to-one reconciliation between deployment/usage records and purchase/license records currently does not exist at NASA. In our view, implementing a centralized Software Asset Management tool and repository—a 'single source of truth' for all software entitlements—is crucial to correcting licensing deficiencies and controlling costs.

Comprehensive Software Management Policy Lacking

NASA's Software Asset Management policy—the business rules and guidelines for managing IT assets throughout their life cycles—is not comprehensive or standardized, leaving roles, responsibilities, and processes unclear. Specifically, NASA does not have enterprise-wide policies, procedures, and requirements addressing software license management. Although NASA implemented a policy on these issues in July 2017 that has since been updated multiple times, it still lacks clear direction and organizational alignment.[22]

The current policy places responsibility for software engineering requirements within the Office of the Chief Engineer. Although the NASA CIO has institutional authority for all Agency-wide enterprise applications such as SAP, WebTADS (employee time and attendance system), and ConcurGov (employee government travel system), clearly defined roles and responsibilities are absent from the policy. Additionally, this policy does not address software licensing and tracking for either commercial or internally developed mission applications. Further, the policy identifies multiple Agency-wide software inventories and repositories, which conflicts with an enterprise-wide centralized software license management approach—a leading best practice that would help manage software licenses. As a result, without a comprehensive software management policy, the Agency lacks an efficient, cohesive, and effective way to manage its software assets across organizational boundaries.

Software Management Function Misaligned

While NASA has engaged in operational planning to standardize the creation of a centralized Software Asset Management program for more than 10 years—with the most recent transformation occurring as part of the Mission Support Future Architecture Program initiative—integration efforts remain disjointed.

We found the Agency has failed to adhere to OMB's 2016 memorandum directing the software manager to report to the agency CIO and work collaboratively with financial, legal, and other organizations as

[22] NASA's current software policy is NASA Procedural Requirements 7150.2D.

appropriate.[23] Specifically, as of October 2021 the Software Asset Management Office and its Agency Software Manager report to the newly created Enterprise Business Management Office, which manages the OCIO's investments and resources and falls under the Strategy Division. While this may initially have a positive effect on the Software Asset Management Office's ability to access some of the Agency's financial resources, the Enterprise Business Management Office is at a tertiary tier under the CIO and is not optimally aligned to work with the Operations Division, which is responsible for program and project management and IT services such as cloud computing. Moreover, this alignment does not meet the intent of OMB and may prove problematic when considering other core competencies of the Software Asset Management program, such as effective software deployment processes and accurate inventories. As a result, despite OMB's policy requiring the Agency Software Manager to report to the CIO, the Software Asset Management Office remains misaligned—likely limiting its ability to successfully influence and navigate the complexities of software management across organizational boundaries.

Ad Hoc Legal Consultation

NASA does not have a consistent, Agency-wide process for including legal representation during software contract negotiations and vendor audits. Instead, Agency officials explained that the process for engaging legal counsel varies greatly from Center to Center and organization to organization. While the NSSC provides a contract legal sufficiency review (e.g., terms and conditions), NASA's Office of General Counsel is only required to be involved when software contracts exceed a $1 million threshold.

Likewise, legal involvement in vendor audits is ad hoc and most often at the discretion of the Agency organization under audit. In fact, we were told that many times Agency lawyers are unaware a software audit is transpiring and are not engaged unless a vendor claim is submitted to NASA. For example, in January 2021 the vendor SUSE contacted Ames Research Center's supercomputing group requesting they run a script to confirm use of their software on NASA systems. The supercomputing group complied and only when confronted with an unexpected $7 million invoice from SUSE did they engage Ames Research Center's Office of General Counsel, OCIO, and the Office of Procurement for assistance. At the Office of General Counsel's direction, all conversation with the vendor was halted, forcing the vendor through a more formalized audit process. However, since the script data was provided before legal involvement, financial penalty negotiations were considerably more difficult and Ames ended up reimbursing SUSE $3.8 million. In our view, engaging legal counsel early may minimize the complexity and pitfalls of alleged deficiencies in licensing records, including limiting financial penalties.

Similarly, in July 2019 the vendor SAP approached Goddard Space Flight Center's Astrophysics Division and requested data regarding product usage. The organization complied, but eventually realized it was a mistake to provide that information directly to the vendor before engaging Agency legal counsel. However, only when the Office of Procurement received an unanticipated invoice for $415,000 did OCIO Headquarters officials and the Office of General Counsel become involved to assist with financial penalty negotiations. Because a majority of software contracts include a *right to audit* clause, there is no requirement for the vendor to provide anything other than a legal notice by letter about the initiation of an audit and a reasonable timeframe for the licensee to prepare for the audit. Without a formal process for how and when to engage legal counsel in such situations, NASA remains at risk of vendor audits resulting in license non-compliance and will continue to be subject to significant monetary violation penalties.

[23] OMB Memorandum M-16-12.

Inconsistent Training

We found training for software license use and management inconsistent across NASA. Although the Agency has established 2 hours of web-based training, the content is more than 5 years old.[24] Created in 2017, the course provides technical training for the phases of software life-cycle management (plan, acquire, use, manage, and dispose), as well as topics such as intellectual property, contracts, negotiations, compliance, audits, security, configuration management, and services such as Software as a Service.[25]

During our analysis of data from the System for Administration, Training, and Educational Resources (known as SATERN), we found that 843 individuals completed the course between November 2017 and March 2022. This training appears to be randomly assigned to engineers and others and is not routinely required for officials who have direct and regular involvement with the purchase or management of software such as legal, procurement, Center IT asset managers, and system administrators.

While in-depth training on Software Asset Management practices is important for specific job functions such as IT managers, in our view more general training could enhance the workforce's knowledge of software licensing—potentially avoiding unintended consequences of license violations such as downloading 'free' software to the NASA network. Although many times 'free' software is available for individual use, it is not commonly permitted for Agency or corporate use. For example, Oracle's VirtualBox can be downloaded and used for free by personal users.[26] However, agencies and corporate users such as NASA must purchase the VirtualBox Extension Pack Enterprise commercial license for business use. Without a brief software licensing overview course as part of all employees' annual training, the workforce lacks the general awareness needed to prevent potential license misuse and subsequent monetary penalties for using software meant for personal not business use.

Lack of Insight on Spending and Software License Violation Penalties Creates Financial Risks

NASA has not implemented the processes necessary to appropriately manage financial risks related to Software Asset Management. Specifically, we found the Agency lacks insight into its software spending as software purchases are not sufficiently tracked, leading to penalties that cost the Agency millions of dollars. Within NASA's FY 2022 $2 billion-plus IT budget, OCIO's software budget was just under $300 million. However, the OCIO's insight into and control over the bulk of the Agency's IT funding remains limited, with the Mission Directorates and Centers independently controlling more than half of this total in their respective budgets. Although NASA tracks some software spending, it is not a discrete or centralized process. We found that data from disparate sources, such as IT, procurement, and finance, are not integrated and do not contain enough detail to accurately determine what software was

[24] The *NASA Software License Management* web-based training course in NASA's System for Administration, Training, and Educational Resources (SATERN)—the Agency's Learning Management System—provides information on NASA Software License Management.

[25] Software as a Service, or SaaS, is a way of delivering applications remotely over the internet instead of installing them locally on computers. With a licensing model resembling paying rent, Microsoft's Office 365 is an example of SaaS.

[26] VirtualBox works by extending the capability of the existing operating system, allowing it to run virtual machines without any changes to hardware or software configuration.

purchased.[27] Further, IT spending data is hampered by a lack of insight into software acquired by purchase cards, which allows individuals to pay for approved purchases of supplies, services, or construction. For example, while existing software standards support enterprise and desktop purchases, the lack of a comprehensive policy allows some users to bypass OCIO authorization (and Software Asset Management team scrutiny) to purchase business and engineering software through alternative means such as purchase cards. As a result, compiling a complete and accurate report of annual software spending is a significant, often manual effort.

Additionally, NASA has historically experienced a large influx of software into its network environment that is not sufficiently tracked for license compliance. Collectively, over the past 5 years the Agency has encountered more than $20 million in unplanned software expenses through penalties and true-ups/ vendor audits.[28] For example, in FY 2017 IBM conducted a software audit resulting in an $18.9 million expense to the Agency to bring NASA's software usage in compliance with license agreements. Similarly, in FY 2021*, known* vendor software settlements equated to almost $4.4 million, as shown in Table 1.

Table 1: FY 2021 Software License Violation Penalties

Software	NASA Center	Finding	Settlement	Status
Ansys	Agency	$959,051.00	$0.00	Completed
Dassault	Agency	$1,201,223.44	$90,000.00	Completed
OpenText	Langley	$8,300.00	$8,300.00	Completed
PTC Windchill	Agency	$3,500,000.00	$0.00	Completed
SAP	Goddard	$415,054.15	$415,054.15	Payment in-process
SAP	Marshall	$205,000.00	$0.00	Completed
SUSE	Ames	$7,000,000.00	$3,846,736.32	Completed
		Total Settlement	**$4,360,090.47**	

Source: NASA OIG representation of Agency data.

Note: Agency refers to the entire NASA organization. Goddard Space Flight Center (Goddard), Marshall Space Flight Center (Marshall), Ames Research Center (Ames), and Langley Research Center (Langley). There is often a significant difference between a vendor software penalty *Finding* and NASA *Settlement* due to resolution options such as early license renewal or the purchase of additional software.

Because the Agency does not have a method for tracking payouts for software license infractions in SAP—NASA's financial management system— the magnitude of vendor software settlement payments is unknown. True-ups are normally paid through institutional or mission program funds and identified as 'IT spend' in lieu of 'penalty spend' in SAP. Without visibility into unplanned software expenses, the Agency has no comprehensive insight into the size of such penalties, although as evidenced by the limited information on FY 2021 payouts, the amount is in the millions of dollars. Notably, as of August 2022, Agency officials informed us the Office of the Chief Financial Officer has agreed to explore implementing a "penalty spend" classification in SAP to track license infraction and true-up payouts.

[27] We were unable to determine the reliability of the data for software spending and therefore the magnitude of the issues identified may be greater than reported.

[28] These penalties are for known large scale audits managed within the OCIO and NSSC. Insight into Agency-wide software penalties are unknown. True-up is the yearly vendor evaluation of qualified software licenses deployed within an organization.

Based on the data available, we found that in excess of $20 million has been unnecessarily spent on software fines and penalties over the last 5 years. In our judgement, penalty expenditures were potentially avoidable if an enterprise-wide Software Asset Management program had been operational. Therefore, we are questioning the $20 million in penalties. See Appendix D for a detailed explanation of these questioned costs. Indeed, those funds could have been put to better use, easily offsetting budget shortages and the estimated $3 million cost to implement and $2.5 million annual cost to sustain a Software Asset Management program within NASA's IT ecosystem.

We estimate the Agency could have saved approximately $35 million over the past 5 years—$20 million in fines and overpayments plus the $15 million spent on unused Oracle licenses—and moving forward, could save approximately $4 million over the next 3 years if the enterprise-wide Software Asset Management program and tools are operational. Appendix D provides additional details and the calculations we used to determine how funds could be put to better use.

Privileged Access Exposes Potential Cybersecurity Risks

NASA has not implemented the enterprise-wide processes necessary to appropriately manage cybersecurity risks related to Software Asset Management. Specifically, we found software downloaded with privileged access is not tracked for license compliance and life-cycle management and may inadvertently introduce cyber vulnerabilities including malware into NASA networks.[29] Likewise, NASA does not have a consistent, Agency-wide process for limiting privileged access to computers—a bedrock cybersecurity principle.[30] The concept of 'least privilege'—granting a user only those permissions needed to perform their job—is a key cybersecurity component for the management of software and IT assets.

Any software deployed within the Agency, regardless of its function, injects risk into NASA's infrastructure from a cybersecurity and software license compliance perspective.[31] Importantly, cyber risk is heightened when privileged users have unfettered access to IT systems. Privileged access in the hands of malicious actors can inflict significant damage such as ransomware attacks, data theft, espionage, or sabotage by bypassing important safety access controls.[32]

We found that over the last 15 years, through three enterprise-wide IT management contracts, NASA has struggled to gain control over the use of privileged access.[33] While some progress has been made on NASA's institutional systems, as many as 60 percent of one NASA Center's assets are managed by Mission Directorates and are therefore outside the OCIO's purview and the software life-cycle process.[34]

[29] Malware is a program, such as a virus, Trojan horse, or spyware, inserted into a system, often covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system.

[30] A privileged user has more IT system authority than an ordinary, non-privileged user. For example, privileged users might be able to install or remove software, upgrade the operating system, or modify application configurations. Also, they might have access to files that are not normally accessible to non-privileged users.

[31] NASA is aware of the cybersecurity concerns associated with software management; this report, however, focuses on specific operational and financial Software Asset Management risks.

[32] Ransomware is designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption.

[33] These three contracts provide Agency-wide IT services for basic hardware and software computing services: (1) Outsourcing Desktop Initiative for NASA (ODIN), awarded in 2004; (2) Agency Consolidated End-User Services (ACES), awarded in 2010; and (3) NASA End-user Services & Technologies (NEST), awarded in 2019.

[34] The names of NASA Centers are generalized to protect operational cybersecurity.

In our analysis, data indicated that between 2020 and 2022 almost 11,000 users Agency-wide were granted privileged access, primarily to install software.[35] Alarmingly, we identified that *all* of another NASA Center's approximately 6,500 users have been granted privileged access to their computers—essentially, including the ability to download and install software at will. According to Center and OCIO officials, this carte blanche access was given at this one Center because Center management felt the cost of provisioning elevated privilege requests did not warrant the investment of OCIO resources.[36]

OCIO officials further explained that while the use of privileged access by approximately 6,500 users at a Center has received scrutiny over the years, operational constraints, conflicts due to the complexity and scale of NASA's federated environment, and funding continue to delay restrictions on privileged access.[37] As we have reported in the past, a fragmented approach to IT governance with numerous, separate lines of authority (institutional versus mission) has long been a defining feature of the environment in which cybersecurity decisions are made at the Agency, resulting in a higher than necessary cyber risk. Until NASA takes steps to appropriately limit privileged access and implement Software Asset Management, cyber risk introduced by unauthorized software will remain amplified. Additionally, privileged access increases financial risk because a vendor audit may identify unlicensed software downloaded by a user with privileged access resulting in fines or unplanned expenses.

[35] A majority of privileged access is granted for 30 days or less except in the case of this one Center, where users have maintained privileged access for years.

[36] User provisioning or account provisioning technology creates, modifies, disables, and deletes user accounts and their profiles across IT infrastructure and business applications.

[37] NASA's federated model utilizes decentralized roles and responsibilities for governance of institutional and mission IT.

CONCLUSION

NASA has been slow to formalize its Software Asset Management efforts because of the sheer complexity and volume of its software licensing agreements. Determining a way to harness a better understanding and visibility of current license inventory, promoting a stronger compliance discipline, and reducing costs associated with software license management as a whole has been daunting, and efforts in this direction have been plagued by a series of false starts for more than a decade.

Until NASA addresses the significant weaknesses identified in how it manages the software life cycle, including establishing a centralized and integrated inventory and limiting privileged access, the Agency risks procuring software in a costly and ineffective manner, as well as incurring tens of millions of dollars in penalties for license non-compliance. In our opinion, NASA must act immediately and decisively to deploy a comprehensive Software Asset Management program—managing software with the same rigor and discipline as other Agency expenditures. By minimizing licensing penalties and overspend, the savings could easily offset the cost of implementing a robust program to improve financial accountability and cybersecurity, and avoid more wasteful spending.

Recommendations, Management's Response, and Our Evaluation

To strengthen operational and cyber aspects of Software Asset Management, we recommended the Chief Information Officer:

1. Establish enterprise-wide (institutional and mission) Software Asset Management policy and procedures.
2. Implement a single Software Asset Management tool across the Agency.
3. Align the Agency Software Manager position to report to the Agency CIO.
4. Establish formal legal representation and guidance for vendor software audits.
5. Establish a software license awareness training 'short course' focusing on approvals, compliance, and other issues a general user might encounter.
6. Implement a centralized repository for NASA's internally developed software applications.
7. Develop an Agency-wide process for limiting privileged access to computer resources in accordance with the concept of least privilege.

To strengthen the financial aspects of Software Asset Management, we recommended the Chief Financial Officer:

8. Implement a "penalty spend" classification in SAP to track license infractions and true-up payouts.
9. Centralize software spending insights to include purchase cards.

We provided a draft of this report to NASA management, who concurred or partially concurred with Recommendations 1, 2, 4, 5, 6, 7, 8, 9. We consider the proposed actions responsive and therefore those recommendations are resolved and will be closed upon completion and verification of the proposed corrective actions. The Agency also partially concurred with Recommendation 3, however, we consider the proposed actions unresponsive. The Agency stated that the Software Asset Manager will establish a regular cadence of reporting to the Agency CIO and senior management boards to provide insight into software management activities. While we appreciate the regular reporting of software management activities, in our view, these communication activities do not substitute the requirement outlined in OMB Memorandum M-16-12, which states "the software manager shall report to the Agency CIO." As a cross-functional effort that can impact and, at times, disrupt status quo licensing across the Agency, a successful Software Asset Management program requires executive-level support for decision-making and active engagement to successfully influence and navigate software management complexities across organizational boundaries. Consequently, this recommendation will remain unresolved pending further discussions with the Agency.

Management’s comments are reproduced in Appendix E. Technical comments provided by management and revisions to address them have been incorporated as appropriate.

Major contributors to this report include Tekla Colón, Mission Support Audits Director; Scott Riggenbach, Assistant Director; Joseph Cook; Linda Hargrove; Jobenia Parker; Christopher Reeves; and Vincent Whitfield. Matt Ward and Lauren Suls provided editorial and graphics support.

If you have questions about this report or wish to comment on the quality or usefulness of this report, contact Laurence Hawkins, Audit Operations and Quality Assurance Director, at 202-358-1543 or laurence.b.hawkins@nasa.gov.

Paul K. Martin
Inspector General

Appendix A: Scope and Methodology

We performed this audit from February 2022 through November 2022 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The scope of our audit was NASA's overall risks associated with Software Asset Management over the past 5 years. Our objective was to determine whether the Agency is managing its software assets in an effective and efficient manner while maintaining compliance with applicable requirements and cybersecurity best practices. Specifically, we examined whether NASA (1) is managing software acquisitions and installations to ensure application of effective procurement and cybersecurity controls, (2) has the capability to effectively inventory and maintain its software asset portfolio, and (3) is managing internal software development activities to ensure duplicative software applications are not developed or licenses purchased when existing software capabilities could fulfill requirements.

Methodology

We divided the audit into three software subject areas: (1) Procurement and Cyber Controls, (2) Inventory Controls, and (3) Internal Software Development Activities.

To gain a holistic view of NASA's Software Asset Management and the broader license and cyber risk landscape, for each subject area we reviewed numerous federal and Agency policies, regulations, guidance, and industry best practices for managing software. We interviewed responsible NASA officials from the NSSC, OCIO, Security Operations Center, Enterprise License Management Team, Office of Procurement, and Office of General Counsel. Additionally, we met with officials from Goddard Space Flight Center and Langley Research Center regarding internal software development activities. Collectively, this informed our understanding and helped us assess the effectiveness of NASA's Software Asset Management activities.

Key work completed for each subject area is highlighted below.

Procurement and Cyber Controls. To determine whether NASA is managing software acquisitions and installations to ensure application of effective procurement and cybersecurity controls, we reviewed and analyzed pertinent documentation to gain an understanding of NASA's software management activities. We researched and analyzed federal and industry best practices and compared them to NASA policy. We engaged analysts with the OIG's Office of Data Analytics to compare elevated privilege requests against user software downloads.[38] Additionally, we examined whether the OCIO has identified and mitigated software management top cyber risks, managed capability gaps, and prioritized investments. Finally, to test third party software patch status, we examined scan data for cyber vulnerabilities.

[38] Privileged users have more IT system authority than ordinary (non-privileged) users. Generally, installing software on Windows computers requires administrator rights (e.g., elevated privileges). Accessing IT systems with elevated user privileges greatly increases the risks of security incidents and of unintended and/or detrimental changes to system configurations.

Inventory Controls. To determine whether NASA has the capability to effectively inventory and maintain its software asset portfolio, we determined whether NASA established a centralized Software Asset Management program. We identified staffing levels, tools, and metrics used to manage and track software inventories and overall license administration. We analyzed NASA's OMB submission of Federal Information Technology Acquisition Reform Act data to validate Agency reporting of comprehensive, regularly updated inventory of software licenses. We selected and analyzed software applications widely used by NASA. We assessed Software Asset Management technical training by taking the course and analyzing data on attendees and their corresponding job responsibilities. We also interviewed key personnel to determine confidence levels in current software inventories. Additionally, we reviewed the Mission Support Future Architecture Program initiative and impact to enterprise-wide software management activities. Lastly, we benchmarked against Software Asset Management practices and toolsets at other agencies.

Internal Software Development Activities. To determine whether NASA is managing internal software development activities to ensure duplicative software applications are not developed or licenses purchased when existing software capabilities could fulfill requirements, we discussed internal software development activities, including new development, with responsible officials. We reviewed the Agency Application Rationalization Tool process. Additionally, we analyzed software requests to determine if they are being properly reviewed.

Assessment of Data Reliability

We used limited computer-processed data extracted from NASA's IT systems during the course of this audit. However, we were unable to compare it with other supporting documents to determine data accuracy, consistency, and reasonableness. The data sources are very disparate and do not contain enough detail to determine what was purchased. Further, IT spend data is hampered by insight gaps into purchase cards, service contracts, and NASA agreements. For this reason, we believe the data obtained for this report is of undetermined reliability and the magnitude of the issues identified may be greater than reported. Specifically, while the data used in this report provides context, it does not provide comprehensive procurement, financial, and software inventory information. In response to our questions, Agency officials told us they do not have total confidence in the data because a single Software Asset Management toolset to discover, inventory, correlate, and normalize license data across organizational boundaries is not available. Additionally, officials explained the Agency lacks a definitive way of knowing what software is internally developed versus vendor provided. While data limitations prevented an adequate assessment of the reliability of Agency software license status, it did not affect our ability to address our audit objectives.

Review of Internal Controls

We assessed internal controls and compliance with laws and regulations to determine NASA's overall Software Asset Management. Control weaknesses are identified and discussed in this report. Our recommendations, if implemented, will improve those identified weaknesses.

Prior Coverage

During the last 6 years, the NASA OIG has issued two reports containing some relevance to the subject of this audit. Additionally, the Government Accountability Office has issued several ancillary reports of interest to this topic. Unrestricted reports can be accessed at https://oig.nasa.gov/ and https://www.gao.gov/, respectively.

NASA Office of Inspector General

Audit of NASA's Information Technology Supply Chain Risk Management Efforts (IG-18-019, May 24, 2018)

NASA's Efforts to Improve the Agency's Information Technology Governance (IG-18-002, October 19, 2017)

Government Accountability Office

Software Development: DOD Faces Risks and Challenges in Implementing Modern Approaches and Addressing Cybersecurity Practices (GAO-21-351, June 23, 2021)

Information Technology: DOD Needs to Fully Implement Program for Piloting Open-Source Software (GAO-19-457, September 10, 2019)

Information Technology Reform: Agencies Need to Improve Certification of Incremental Development (GAO-18-148, November 7, 2017)

Information Technology: Agencies Need to Improve Their Application Inventories to Achieve Additional Savings (GAO-16-511, September 29, 2016)

Appendix B: Glossary of Software Products

The below list provides an overview of software products and vendors mentioned in this report.

Adobe. Specializes in software products used across all types of print and electronic media. Known for its multimedia and creativity software, popular products include Photoshop, Acrobat Reader, and Adobe Creative Cloud.

Amazon Web Services. The world's most comprehensive and broadly adopted cloud computing provider. Offered from data centers globally, Amazon's cloud computing provides on-demand delivery of IT resources over the internet with pay-as-you-go pricing. Instead of buying, owning, and maintaining physical data centers and servers, users can access technology services, such as computing, storage, and databases, on an as-needed basis.

Ansys. A general-purpose, finite-element modeling software package for numerically solving a wide variety of mechanical problems such as structural analysis, heat transfer, and fluid systems, as well as acoustic and electromagnetic problems.

BigFix. A centralized operating system patch management service used to provide cyber vulnerability visibility and manage patch compliance.

Dassault. A software company that specializes in 3D design and product life-cycle management software. Flagship products CATIA and SolidWorks are used in aviation and aerospace design, simulation, and manufacturing.

IBM. A global technology company that provides hardware, software, cloud-based services, and cognitive (data analytics) computing. The IBM product families include Maximo, Business Analytics, Tivoli, and WebSphere.

Linux. A free operating system that runs most of the internet, all of the world's top 500 supercomputers, and the world's stock exchanges. Linux may be installed on an unlimited number of computers without paying for software or server licensing.

MATLAB. A programming platform used to analyze data, develop algorithms, and create models and applications.

Microsoft. As the largest software company in the world, Microsoft provides a multitude of operating systems, server applications, software development, and cloud enterprise technology and services. Familiar products include the Windows operating system and Microsoft Word.

Node.js. An open-source development platform for executing JavaScript code on the server. Node.js is useful for developing applications that require a persistent connection from the browser to the server and is often used for real-time applications such as chat, news feeds, and web push notifications.

OpenText. A group of content management software whose programs include document management, record management, email management, and web content management.

Oracle. A relational database management system used to store and retrieve related information. The database has logical and physical structures for data.

PTC Windchill. Provides a systematic approach for creating, configuring, managing, and reusing product structures and associated content, such as computer-aided design files, documentation, requirements, manufacturing information, service information, part and supplier data, calculations, and illustrations.

SAP. An enterprise resource planning system used to streamline business processes. Modules include functions such as human resources, finance, and procurement.

Splunk. A software platform to search, analyze, and visualize machine-generated data gathered from the websites, applications, sensors, and devices that make up the IT infrastructure.

SUSE. A version of the Linux operating system. It assembles the Linux kernel and other open-source components into a full-featured operating system available for purchase.

Symantec Endpoint Protection. Endpoints are a primary target of cyber attackers. Symantec Endpoint Security prevents, hardens, detects, and responds to emerging threats across laptops, desktops, tablets, mobile phones, servers, and cloud workloads.

APPENDIX C: SOFTWARE ASSET MANAGEMENT MATURITY AND OPTIMIZATION MODEL

The *Software Asset Management Maturity and Optimization Model* provides organizations with a way to benchmark their current ability to manage software (see Table 3 on the following page). As indicated on the table, the model classifies Software Asset Management into 10 key competencies, each given one of four possible ratings—Basic, Standardized, Rationalized, or Dynamic. We highlight our assessment of NASA's Software Asset Management competency level in orange and blue text, representing Basic and Standardized ratings, respectively, and found the Agency's overall rating is *Basic*. Clearly, a basic, ad hoc approach presents numerous risks, adds to costs, and is likely unsustainable.

- *Basic.* Software is managed on an ad hoc basis with few, if any, comprehensive policies.
- *Standardized.* The agency uses a discovery tool or data repository for tracking assets, although the information may not be complete or accurate enough for decision-making.
- *Rationalized.* Assets are actively managed, and the agency has put in place policies, procedures, and tools integrated into the full IT asset life cycle.
- *Dynamic.* Assets are optimized, with near real-time alignment with changing business needs.

Table 3: Software Asset Management Maturity and Optimization Model

Key Competency	Basic	Standardized	Rationalized	Dynamic
SAM Throughout Organization	**SAM Manager assigned but roles and responsibilities not defined.**	Direct SAM responsibility is identified throughout the organization.	Each functional group actively manages SAM.	SAM responsibilities defined in job descriptions across organization.
SAM Improvement Plan	**No SAM development or communication plan.**	SAM plan is defined and approved.	SAM improvement is demonstrated.	SAM goals part of executive scorecard; reviewed regularly.
Hardware and Software Inventory	No centralized inventory or < 68% assets in central inventory.	**Between 68% and 95% of assets in inventory.**	Between 96% and 99% of assets in inventory.	99% of assets in inventory.
Accuracy of Inventory	Manual inventory; no discovery tools.	**Inventory sources reconciled annually.**	Inventory sources reconciled quarterly.	Dynamic discovery tools provide near real-time deployment details.
License Entitlement Records[a]	**Procurement manages contracts; not accessed by IT managers.**	Complete entitlement records exist across organization.	Entitlement records reconciled with vendor records.	SAM entitlement system interfaces with vendor entitlement to track usage.
Periodic Evaluation	**IT operations managed on an ad hoc basis.**	Annual sign-off on SAM reports.	Quarterly sign-off on SAM reports.	System reconciliations and ITAM report available on demand.
Operations Management Interfaces	**SAM is not considered part of risk plan and organization integration.**	Operations manage separate asset inventories.	Operations manage associated asset inventory.	All business units follow the same strategy, processes, and technology for SAM.
Acquisition Process	Assets purchased on a per project basis; without a review of current availability.	**Software purchases use approved vendors.**	Software purchases based on deployment/entitlement reconciliation.	All purchases are made using a pre-defined asset catalog; based on metered usage.
Deployment Process	**Assets deployed by end-users in distributed locations; no centralized IT.**	Only approved software is deployed.	Software deployment reports are accessible to stakeholders.	Software is dynamically available to users on demand.
Retirement Process	**Software is retired with hardware and is not harvested or reassigned.**	Unused software is harvested (where the license allows) and tracked within a centrally controlled inventory.	Centrally controlled inventory of harvested licenses is maintained and available for reuse. Deployment and license records are updated.	Automated process with centralized control and tracking of all installed software, harvest options, internal reassignment, and disposal.

Source: NASA OIG representation of the Microsoft Software Asset Management Maturity Model as adopted from International Organization for Standardization/International Electrotechnical Commission 19770-1:2012 Software Asset Management processes.

Note: Software Asset Management (SAM) and Information Technology Asset Management (ITAM).

[a] Similar to a license, an entitlement is the right to use and/or access software as defined through agreement(s) with the software vendor.

Appendix D: Questioned Costs and Funds Put to Better Use

During our review of NASA's Software Asset Management, we questioned costs unnecessarily spent on hefty fines and penalties over the last 5 years and determined those funds could have been put to better use. While penalties are *known* for large scale vendor audits within OCIO and the NSSC, insight into *all* software penalties Agency-wide are unknown, and therefore not included in our estimates.[39] Additionally, the Oracle license overspend has been in effect for more than a decade—since the end of the Space Shuttle program in 2011; the Agency has not sufficiently tracked the full cost of license expenditures for the life of the existing contract which includes multiple option years in a manner which would allow the full costs to be known.

Our *questioned costs* identify costs that appear unnecessary or unreasonable. Similarly, the *funds put to better use* recommendation estimates that funds could be used more efficiently. For example, funds put to better use could result in significant reductions in penalty spending and avoidance of unnecessary software license overspending.

Consequently, we estimate the Agency could have saved approximately $35 million over the past 5 years in fines and overpayments ($20 million in penalties plus $15 million in Oracle overspend) and are therefore questioning these costs. Moving forward, we estimate the Agency could save approximately $4 million over the next 3 years if the enterprise-wide Software Asset Management tools are operational. Specifically, had the Agency not spent $4 million per year in penalties they would have saved $12 million over 3 years. Taking into account implementation and operating costs of a Software Asset Management tool is approximately $8 million (implementation costs of $3 million plus operating costs of $2.5 million for 2 years), $12 million less $8 million is a total of $4 million in funds put to better use.

Table 4 summarizes the questioned costs and funds put to better use identified during our audit and discussed in this report.

Table 4: Summary of Questioned Costs and Funds Put to Better Use

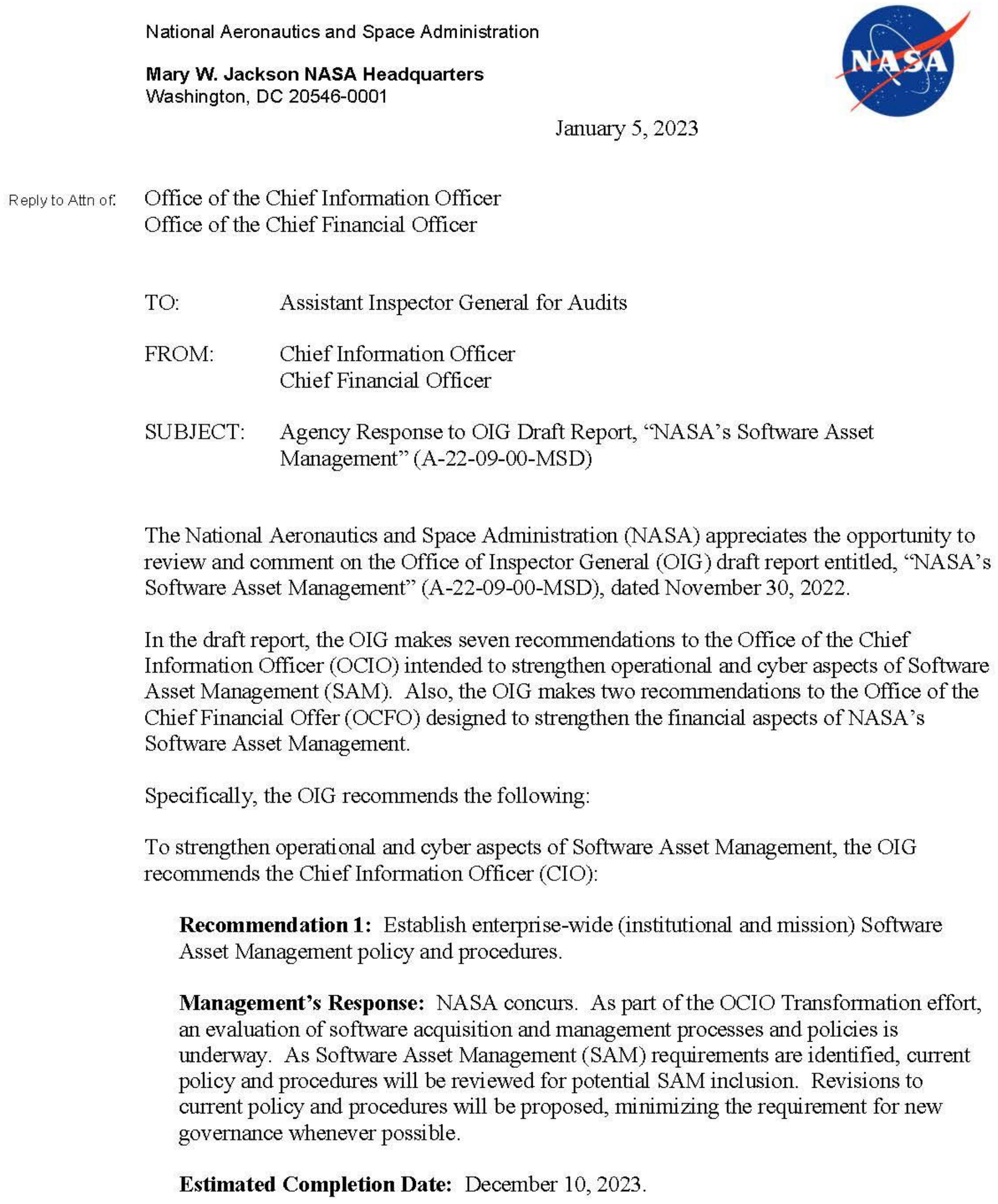
Issue	Recommendation Number	Questioned Costs[a]	Funds Put to Better Use[b]
Unnecessary penalties and Oracle overspend	2 and 8	$35,000,000	N/A
Implement a single Software Asset Management tool across the Agency	2	N/A	$4,000,000

Source: NASA OIG analysis.

[a] Questioned costs are expenditures that are questioned by the OIG because of alleged violation of law, regulation, or contractual requirement governing the expenditure of funds; costs that are not supported by adequate documentation at the time of our audit; or are unallowable, unnecessary, or unreasonable.
[b] Funds put to better use are funds that could be used more efficiently if the Agency takes action to implement and complete the recommendations made by the OIG.

[39] IBM and SAP are examples of large vendors.

Appendix E: Management's Comments



National Aeronautics and Space Administration

Mary W. Jackson NASA Headquarters
Washington, DC 20546-0001

January 5, 2023

Reply to Attn of: Office of the Chief Information Officer
Office of the Chief Financial Officer

TO: Assistant Inspector General for Audits

FROM: Chief Information Officer
Chief Financial Officer

SUBJECT: Agency Response to OIG Draft Report, "NASA's Software Asset Management" (A-22-09-00-MSD)

The National Aeronautics and Space Administration (NASA) appreciates the opportunity to review and comment on the Office of Inspector General (OIG) draft report entitled, "NASA's Software Asset Management" (A-22-09-00-MSD), dated November 30, 2022.

In the draft report, the OIG makes seven recommendations to the Office of the Chief Information Officer (OCIO) intended to strengthen operational and cyber aspects of Software Asset Management (SAM). Also, the OIG makes two recommendations to the Office of the Chief Financial Offer (OCFO) designed to strengthen the financial aspects of NASA's Software Asset Management.

Specifically, the OIG recommends the following:

To strengthen operational and cyber aspects of Software Asset Management, the OIG recommends the Chief Information Officer (CIO):

Recommendation 1: Establish enterprise-wide (institutional and mission) Software Asset Management policy and procedures.

Management's Response: NASA concurs. As part of the OCIO Transformation effort, an evaluation of software acquisition and management processes and policies is underway. As Software Asset Management (SAM) requirements are identified, current policy and procedures will be reviewed for potential SAM inclusion. Revisions to current policy and procedures will be proposed, minimizing the requirement for new governance whenever possible.

Estimated Completion Date: December 10, 2023.

Recommendation 2: Implement a single Software Asset Management tool across the Agency.

Management's Response: NASA partially concurs. NASA is in the process of piloting a SAM tool. The initial implementation is being conducted in a scaled-back manner due to limited licensing and complex integrations. Upon successful completion of the pilot, the intent is to strategically scale this capability to support the enterprise through a common tool, practices, and governance. After scaling to Agency-wide implementation, 85 percent of NASA endpoints will be supported with the SAM Pro tool, which will strengthen the Agency's ability to realize Federal and NASA software asset management directives and goals. There will always be a number of systems operating outside of the NASA network, which will prevent achieving 100 percent automated visibility by the Agency SAM tool.

Estimated Completion Date: The expected completion date for the SAM pilot implementation is October 2, 2023. Scaling to enterprise is dependent on a successful pilot and will require a phased, multi-year effort with an anticipated completion date of October 1, 2027.

Recommendation 3: Align the Agency Software Manager position to report to the Agency CIO.

Management's Response: NASA partially concurs. The Agency Software Asset Manager will establish a regular cadence of reporting to the Agency CIO and senior OCIO management boards through standard OCIO reporting channels and methods. Doing so will provide the Agency CIO with insight into software management activities without adding an additional direct report.

Estimated Completion Date: February 1, 2023.

Recommendation 4: Establish formal legal representation and guidance for vendor software audits.

Management's Response: NASA concurs. In connection with ongoing work to refine Commercial IT Management (CITM) and Software License and Asset Management (SLAM) procedures, OCIO will require that all audit notices and requests be shared with a specified contact point in the Office of General Counsel to ensure that appropriate legal advice and representation are obtained with respect to audit activities.

Estimated Completion Date: June 30, 2023.

Recommendation 5: Establish a software license awareness training 'short course' focusing on approvals, compliance, and other issues a general user might encounter.

Management's Response: NASA concurs. OCIO will develop a short training course for the NASA workforce, focused on enhancing general knowledge of software licensing and the potential for unintended consequences.

Estimated Completion Date: October 2, 2023.

Recommendation 6: Implement a centralized repository for NASA's internally developed software applications.

Management's Response: NASA concurs. OCIO will coordinate with the Office of the Chief Engineer (OCE) to update NASA Procedural Requirements (NPR) 7150.2D, *NASA Software Engineering Requirements*, to require mandatory reporting and inventory of internally developed software applications using the Agency Application Rationalization Tool (AART). This will allow for the use of AART to be more consistent across the Agency.

Estimated Completion Date: October 31, 2024.

Recommendation 7: Develop an Agency-wide process for limiting privileged access to computer resources in accordance with the concept of least privilege.

Management's Response: NASA concurs. OCIO will develop an Agency-wide process for limiting privileged access to computer resources in accordance with the concept of least privilege. Specifically, NASA will collect use cases and develop a process that is practical and feasible while enhancing security and minimizing impact on information technology operations.

Estimated Completion Date: December 1, 2023.

To strengthen the financial aspects of (SAM), the OIG recommends the Chief Financial Officer:

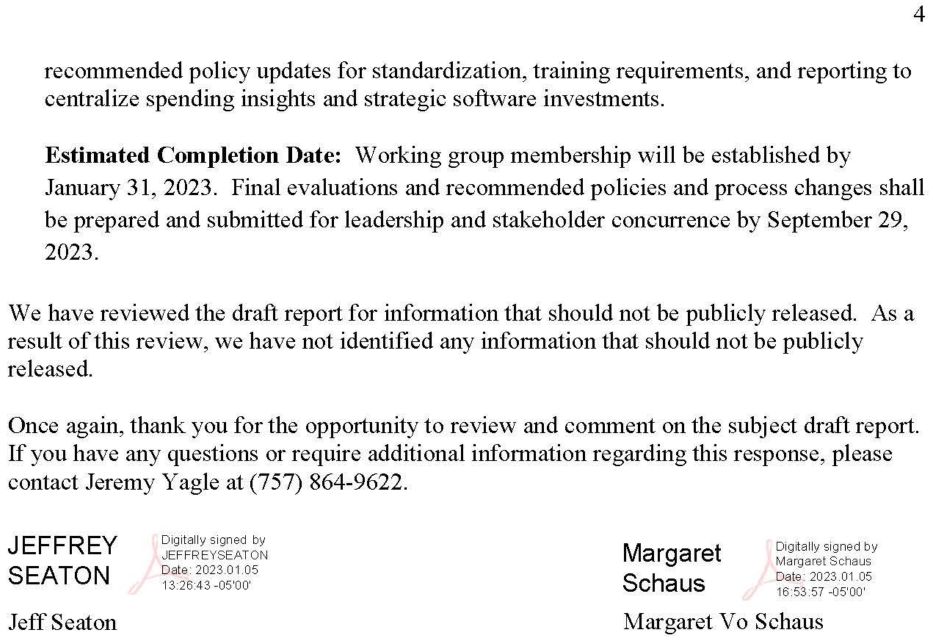
Recommendation 8: Implement a "penalty spend" classification in SAP to track license infractions and true-up payouts.

Management's Response: NASA concurs. Two new classification codes have been added to SAP to facilitate tracking of licensing infractions and true-up payouts. Personnel will receive guidance on the use of these designated codes.

Estimated Completion Date: January 31, 2023.

Recommendation 9: Centralize software spending insights to include purchase cards.

Management's Response: NASA concurs. A cross-functional working group will be established with OCIO, OCFO, and Office of Procurement membership. The working group will evaluate Agency spending and acquisition processes for software, and provide



4

recommended policy updates for standardization, training requirements, and reporting to centralize spending insights and strategic software investments.

Estimated Completion Date: Working group membership will be established by January 31, 2023. Final evaluations and recommended policies and process changes shall be prepared and submitted for leadership and stakeholder concurrence by September 29, 2023.

We have reviewed the draft report for information that should not be publicly released. As a result of this review, we have not identified any information that should not be publicly released.

Once again, thank you for the opportunity to review and comment on the subject draft report. If you have any questions or require additional information regarding this response, please contact Jeremy Yagle at (757) 864-9622.

JEFFREY SEATON Digitally signed by JEFFREYSEATON Date: 2023.01.05 13:26:43 -05'00'	Margaret Schaus Digitally signed by Margaret Schaus Date: 2023.01.05 16:53:57 -05'00'
Jeff Seaton	Margaret Vo Schaus

APPENDIX F: REPORT DISTRIBUTION

National Aeronautics and Space Administration

Administrator
Deputy Administrator
Associate Administrator
Chief of Staff
Chief Information Officer
Chief Financial Officer
Deputy Associate Administrator for Business Operations
Executive Director, NASA Shared Services Center

Non-NASA Organizations and Individuals

Office of Management and Budget
Deputy Associate Director, Climate, Energy, Environment and Science Division

Government Accountability Office
Director, Contracting and National Security Acquisitions
Director, Information Technology and Cybersecurity Issues

Congressional Committees and Subcommittees, Chairman and Ranking Member

Senate Committee on Appropriations
Subcommittee on Commerce, Justice, Science, and Related Agencies

Senate Committee on Commerce, Science, and Transportation
Subcommittee on Space and Science

Senate Committee on Homeland Security and Governmental Affairs

House Committee on Appropriations
Subcommittee on Commerce, Justice, Science, and Related Agencies

House Committee on Oversight and Reform
Subcommittee on Government Operations

House Committee on Science, Space, and Technology
Subcommittee on Investigations and Oversight
Subcommittee on Space and Aeronautics

(Assignment No. A-22-09-00-MSD)